Maintenance Manual
Version 1.02

iCT2xx, iPP3xx, iWL2xx and iSMP terminals

PayEx
EXPERTS IN PAYMENTS

Contents

Introduction 4

Terminal overview 5

Terminals 6

Troubleshooting 7

Troubleshooting ECR 7

Troubleshooting TMS 9

Troubleshooting declined transactions 11

Troubleshooting offline transactions 19

Using the Telium manager 21

Blocked terminals 22

Terminal hardware errors 24

Alert irruption 24

Unauthorized 24

Support menu 25

Files on the terminal 27

Communication 28

TMS 28

Parameters for terminals 29

iWL220 29

Appendices 35

Appendix A – Receipt information 35

Appendix B – Response codes 38

Appendix C – TVR and TSI 41

Appendix D – AID 45

Appendix E – Configuration parameters list 46

Appendix F – Supported schemes 49

Appendix H – Accessories 50

Appendix I – Abbreviations and acronyms 51

Notes 52

Change log

Date	Version	Change	Author
03.05.2013	1.0	Initial version	Trond Hagehaugen
21.08.2013	1.01	Improved/added: Troubleshooting, Configuration and Connection parameters. Added transaction types: Preauthorization and Pin Bypass. Added Authorization response codes, Acquiring Bank contact information. Removed LLT chapter.	Trond Hagehaugen
02.04.2013	1.02	Improved/added/removed: Improved flowcharts, fixed tables with wrong information. Added config parameters corresponding to terminal version 2.08, Removed transaction types chapter. Removed terminal properties.	Trond Hagehaugen

Version 1.02 April 2014.

Copyright © 2014 PayEx Norge AS.
All rights reserved. Copying and/or redistribution of this information in whole or in part without the express permission of PayEx Norway AS is prohibited.

Introduction

Thank you for choosing PayEx as service provider for your payment solution.
This manual provides information and guides you through the maintenance procedures associated with 1st Line Support of the PayEx terminal. Read the manual carefully to perform first hand service on the terminal.

This manual is not intended for self-education but prerequisites that proper training has been undergone prior to use of this manual.

PayEx 2nd Line Support can be contacted by using the contact information below. When contacting PayEx 2nd Line Support, please provide as much information about the issue as possible;

- A detailed description of the error and how/if it can be reproduced
- Photo/Scan of the receipt, screenshots/photos/description of what the terminal displays
- PosPay© log (Where applicable. Contact PayEx 2nd Line Support for assistance)
- Terminal log (Where applicable. Contact PayEx 2nd Line Support for assistance)

Contact information PayEx 2nd Line Support

Denmark: Telephone: **+46 498207878** email: **support.pos@payex.com**.
Finland: Telephone: **+46 498207878** email: **support.pos@payex.com**.
Norway: Telephone: **+47 22036004** email: **support.pos@payex.com**.
Sweden: Telephone: **+46 498207878** email: **support.pos@payex.com**.

The contact information above is for PayEx 2nd Line Support only. To purchase terminals and accessories, please contact PayEx via email: order.pos@payex.com.

Contact information Acquiring Bank

For matters regarding settlement, the Acquiring Bank can be contacted by using the contact information below:

Bank/Acquirer	Telephone	Email/contact
Dankort	+45 44892929	http://www.nets.eu/dk-da/Service/kundeservice/betalingskort/Pages/default.aspx
Euroline (SEB)	+46 8146914	euroline@seb.se
Handelsbanken	+46 87016275	kortsupport.inlosen@handelsbanken.se
Nordea	+46 771336699	nordea.com/About+Nordea/Contact/51452.html
Swedbank	+46 84111080	babs.kundservice@swedbank.se
Teller Denmark	+45 44684468	teller.com/dk/kontakt
Teller Norway	+47 81500400	kundeservice-no@teller.com
Teller Sweden	+46 771220055	kundservice-se@teller.com

Terminal overview

PayEx product portfolio consist of high quality products from Ingenico. Payment terminals offered are the iCT-, iPP-, iSMP and iWL-series.
The terminals are delivered with two types of keyboard layout.
1. Keyboard with text on the red (CANCEL or STOP), yellow (CLEAR) and green button (ENTER or OK).
MENU key is used to enter menu on standalone terminals.
2. Keyboard without text on the red, yellow and green button.
F key is used to enter menu on standalone terminals.

Entering menu on ECR connected terminals requires the following key combinations: F3 (up arrow) + operator password (default: 1234) + Green key + 2 (Mynt). Note that the transaction menu is disabled for ECR connected terminals, all financial transactions must be initiated from the ECR.

All terminals are delivered with a preinstalled set of applications.
The terminals are also delivered with a standard administrator and operator code. The administrator code is set default to 1111 and the operator code is set default to 1234. Change these codes as soon as the terminal is installed. The instructions for changing these codes are described in the terminal's user manual.

Terminals

Use the elements in this chapter in order to identify your product.

Display: For iCT220, iPP320, iWL220 and iSMP, the display is Black and White,-50 series are color terminals.

Terminal casing colors:

iCT220 &250: Black

iPP320: Grey, iPP350: Black

iWL220: Black, iWL250: Grey

iSMP: Black

= Locate terminal type.

iCT220 &250

iPP320 & 350

iWL220 & 250

iSMP

Troubleshooting

This chapter will guide you through troubleshooting of the terminal.

Troubleshooting ECR

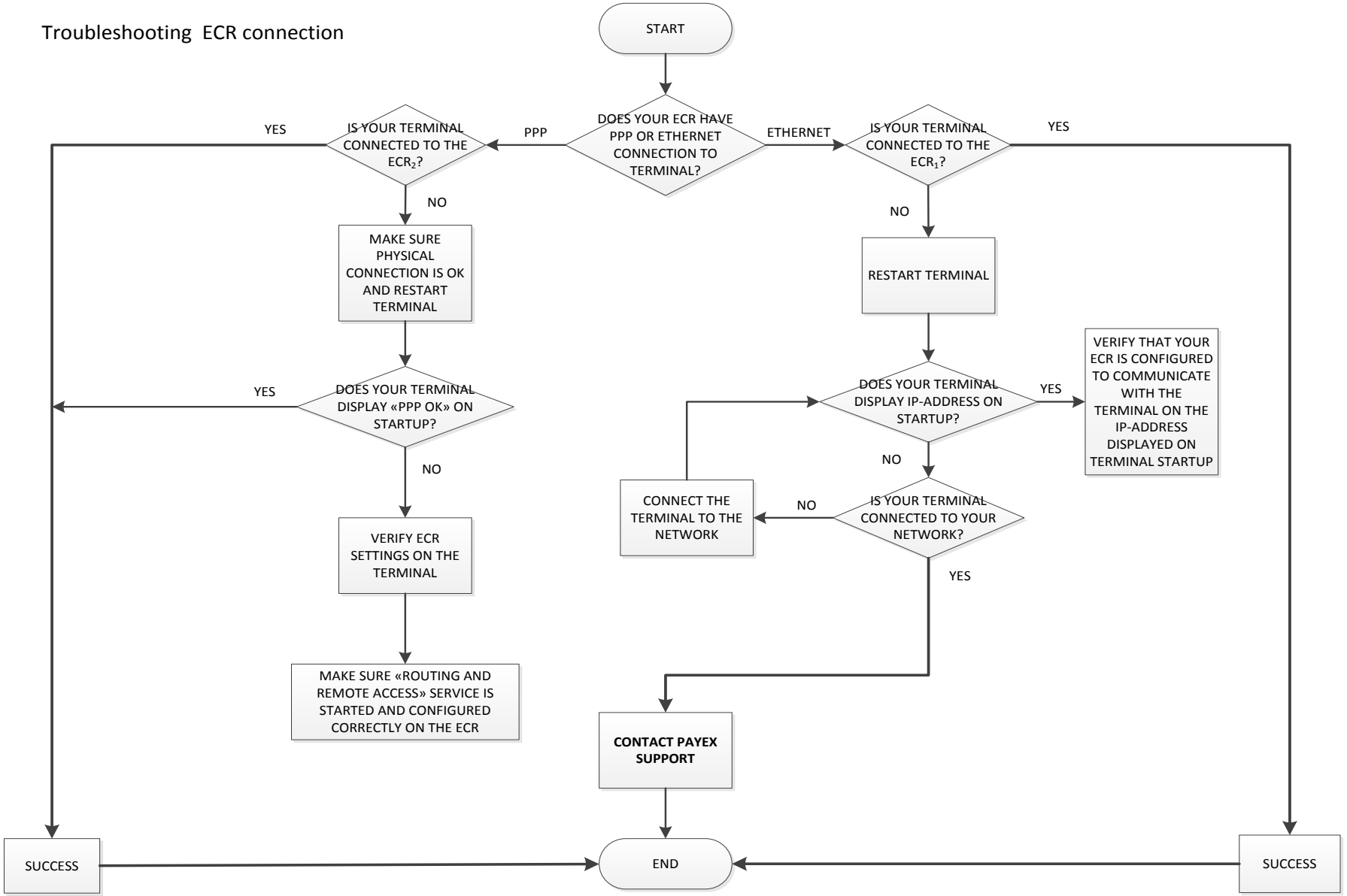
This chapter helps to identify and troubleshoot issues and errors associated with ECR connection. The flowchart on the next page is a flowchart for (re)connecting the terminal to the ECR.

1. The terminal is connected to the ECR if an IP address is displayed in the terminal display and the ECR is configured to communicate with the terminal on that specific address. Terminals configured with static IP-address does not display the IP-address. See the Parameters for terminals chapter for configuring static IP-address.
2. The terminal is connected to the ECR if the terminal displays “PPP OK”. “PPP OK” should be displayed within one (1) minute. If not, restart the ECR and Terminal.

If the terminal is still disconnected after these actions, contact PayEx 2nd Line Support.

Warning! Each version of the software components delivered by PayEx (i.e. payment application in terminal and PosPay© Client) correspond to the other. Always ensure that compatible versions are used before contacting PayEx 2nd Line Support.

Troubleshooting ECR connection


START
DOES YOUR ECR HAVE PPP OR ETHERNET CONNECTION TO TERMINAL?
PPP
ETHERNET
IS YOUR TERMINAL CONNECTED TO THE ECR2?
YES
NO
IS YOUR TERMINAL CONNECTED TO THE ECR1?
YES
NO
MAKE SURE PHYSICAL CONNECTION IS OK AND RESTART TERMINAL
RESTART TERMINAL
DOES YOUR TERMINAL DISPLAY «PPP OK» ON STARTUP?
YES
NO
DOES YOUR TERMINAL DISPLAY IP-ADDRESS ON STARTUP?
YES
NO
VERIFY THAT YOUR ECR IS CONFIGURED TO COMMUNICATE WITH THE TERMINAL ON THE IP-ADDRESS DISPLAYED ON TERMINAL STARTUP
VERIFY ECR SETTINGS ON THE TERMINAL
CONNECT THE TERMINAL TO THE NETWORK
NO
IS YOUR TERMINAL CONNECTED TO YOUR NETWORK?
YES
MAKE SURE «ROUTING AND REMOTE ACCESS» SERVICE IS STARTED AND CONFIGURED CORRECTLY ON THE ECR
CONTACT PAYEX SUPPORT
SUCCESS
END
SUCCESS

Troubleshooting TMS

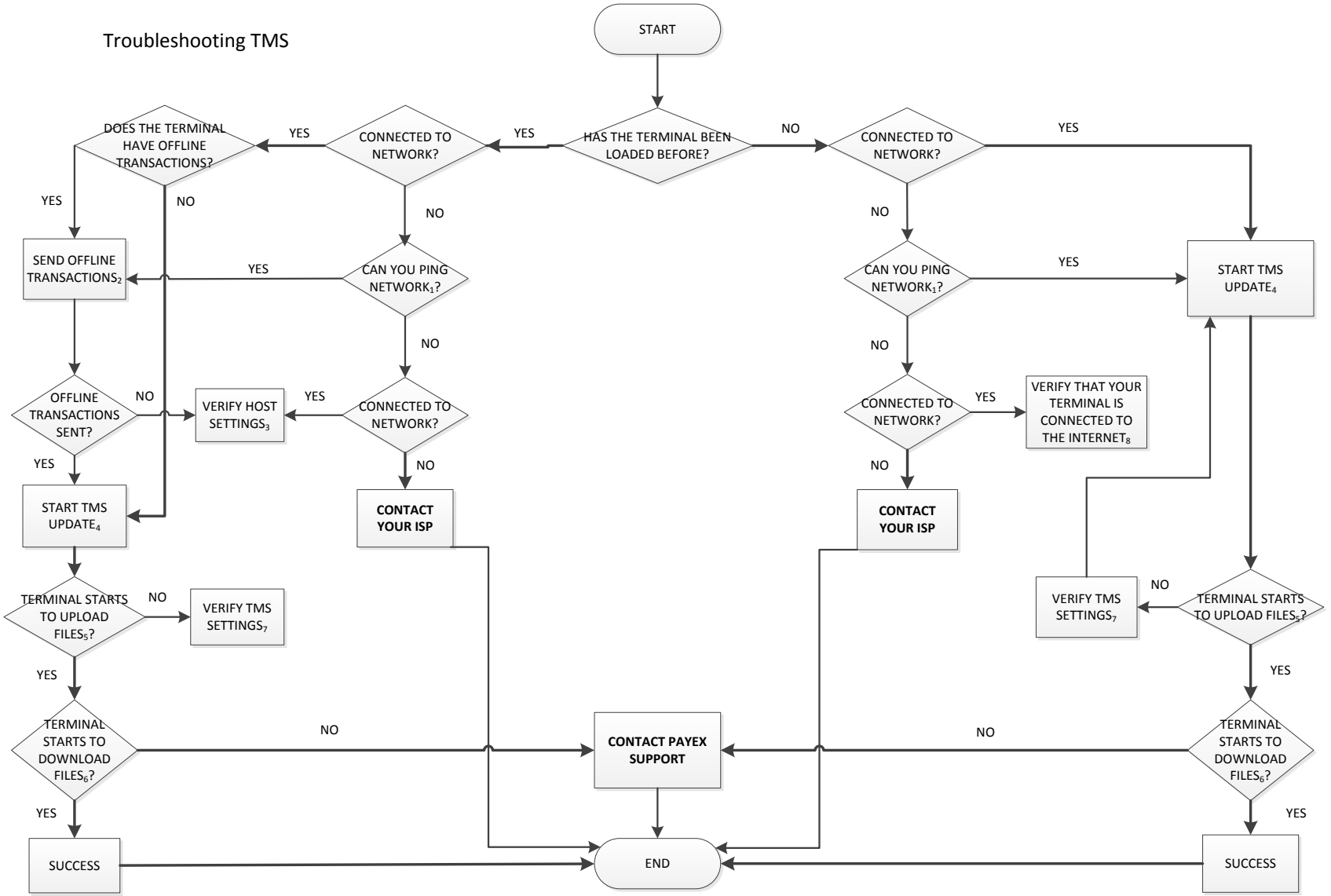
This chapter helps to identify and troubleshoot issues and errors associated with TMS.
The flowchart on the next page is a step-by-step chart of how to download new applications and/or configuration sets from TMS.

1. Ping network: F3+operator code (1234) + TELIUM MANAGER + Initialization + Hardware + Ethernet Setup + Ping. Enter a valid IP-address and press OK. Received packages shall be 4/4. iWL220&250 does not have this property.
2. Send offline transactions: F+4(send offline) or F3+operator password (default 1234)+4(send offline). Offline transaction must be sent before the terminal can perform a TMS update. The terminal will display "Evolution refused" if offline transactions exists.
3. Verify Host settings: Enter support menu and verify parameters by entering the Host connection submenu. Contact PayEx 2nd Line Support if the host connection parameters are configured wrong or to verify that they are correct on the terminal.
4. Start TMS update: Standalone terminals: Start TMS update by entering the system menu; F+7+4. Terminals can also start TMS update from the Telium manager menu, F3+operator code+0+2+2+OK/Green key.
5. Terminal will start to upload files if filenames (i.e. activity.inf) are shown on the terminal display.
6. Terminal will start to download files if filenames are displayed on the terminal display with a progress indicator.
7. TMS settings are located in the Telium Manager menu, F3+0+3+1+T.M.S. Verify that they are correct for the terminal, see the Parameters for terminals chapter.
8. The terminal must have a physical connection to Internet, either via the ECR or via Ethernet with SSL.

iSMP terminal must be connected to the iOS device in order to have an active Internet connection. It is important that the iOS device is connected to the terminal during the whole TMS download. If the iOS device is disconnected from the terminal, the TMS download will not succeed and a new TMS update must be performed. iSMP terminals might need a few attempts to successfully download a TMS package.

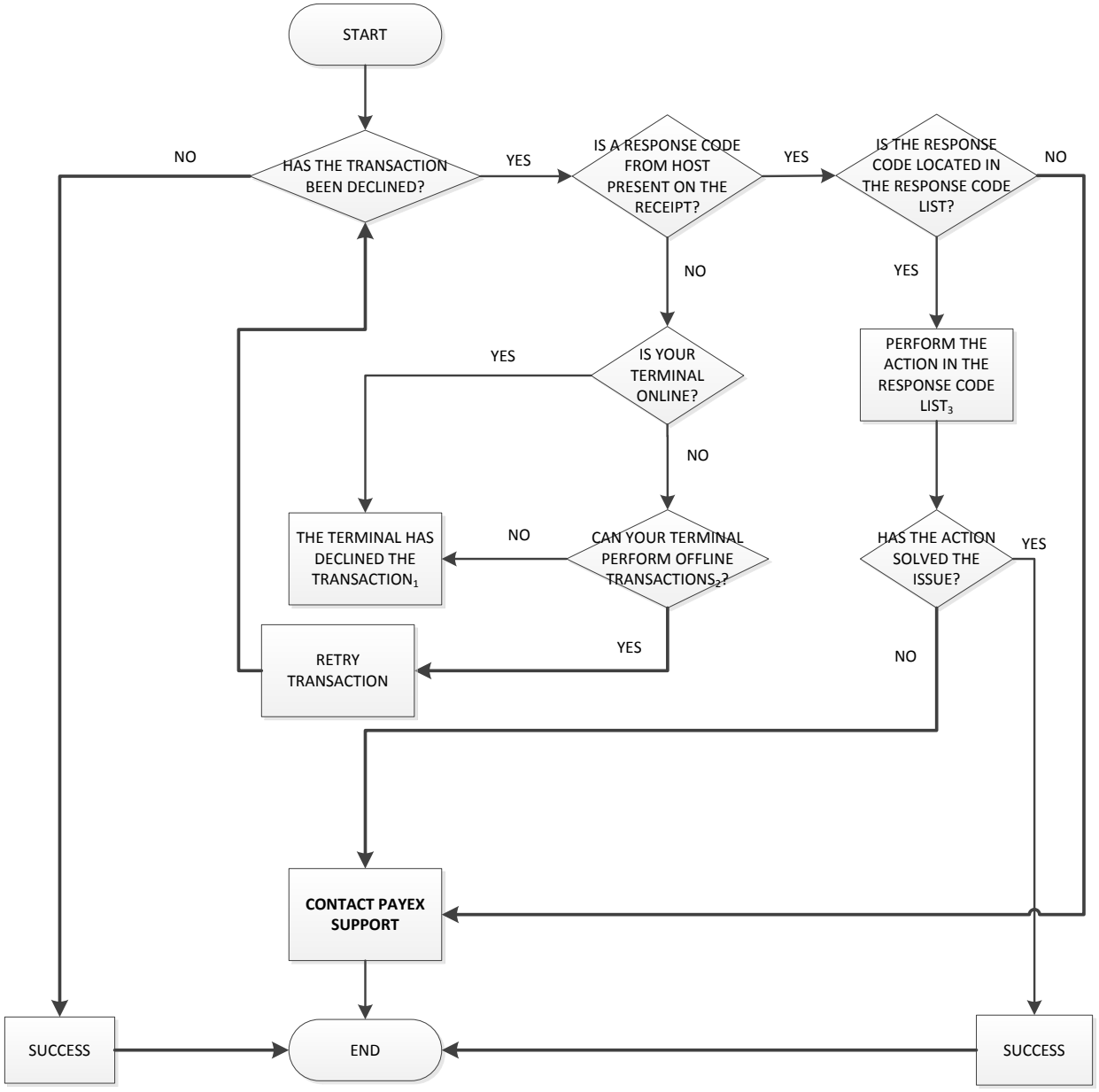
If any action does not solve the issue, contact PayEx 2nd Line Support.

Troubleshooting TMS



Troubleshooting declined transactions

This chapter helps identifying the most common causes for declined transactions.



1. See the Declined transactions chapter on page 12.
2. Online only terminals or transaction types where the terminal is required to be online will always be declined.
3. See the response code list on page 36.

If any action does not solve the issue, contact PayEx 2nd Line Support.

Declined transactions

The most common declined transactions are listed below. For all other declined-situations, contact PayEx 2nd Line Support.

If there is something wrong with the keys in the terminal, it can appear in multiple cases listed below.

All display screenshots on the following pages are based on English setup and can differ from terminal type and setup. Equivalent messages in the local language may be displayed in some occasions.

Card is inserted or swiped and the transaction is declined without PIN entry

Possible issues

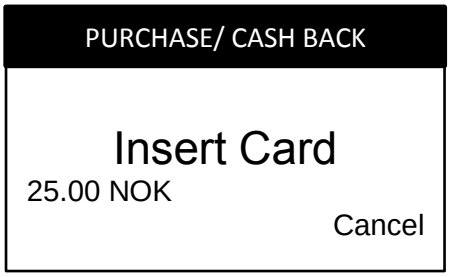
1. The card has a service code that is applicable for ATM's only.
2. The card used (chip card) has been inserted and is not found in the BIN table (See Appendix F – Supported on page 49). The following screenshots will be displayed on the terminal:

Terminal requires that the card is inserted.

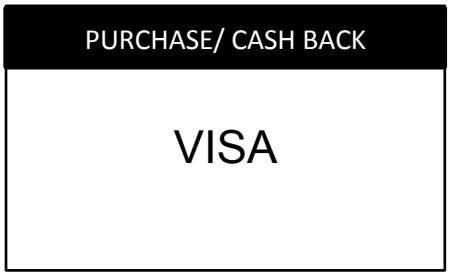
The terminal displays the AID on the chip.

The PAN is not found in the BIN table and the transaction is therefore declined.

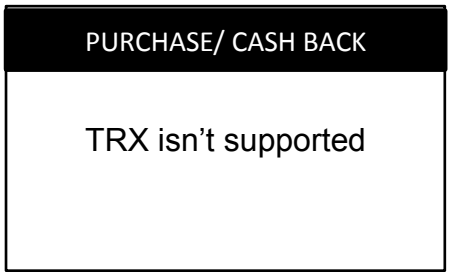
3. The card used is found in the BIN table but the transaction type is not supported, i.e. International card not supporting domestic Cash Back. The following screenshots will be displayed on the terminal:



Terminal requires that the card is inserted.



The terminal displays the application label of the chip.



The PAN is found in the BIN table, but the transaction type for that card is not supported.

4. The following screenshots will appear if one of these error situations occur:
   - Magnetic stripe cards (1st and last screenshot).
   - Chip cards that have been swiped (1st and last screenshot).
   - Chip cards that have been misread multiple times and then terminal requested it to be swiped, called fallback (all screenshots). For fallback transactions, the terminal can also decline the transaction based on:
   - The terminal is configured to decline all fallback transactions
   - Fallback is not allowed for the card used
   - There is something wrong with the keys in the terminal.
   - A chip card that is working and immediately requests fallback might be a result of an unknown card (no record found in EMV.PAR).

Terminal requires that the card is inserted.

Terminal requires that the card is removed because the chip could not be read. Previous and this screenshot will be displayed until the chip is read, or it requires fallback (after 3 attempts).

The terminal requests fallback.

The card is not found in the BIN table and the transaction is declined.

The transaction has been declined after PIN entry

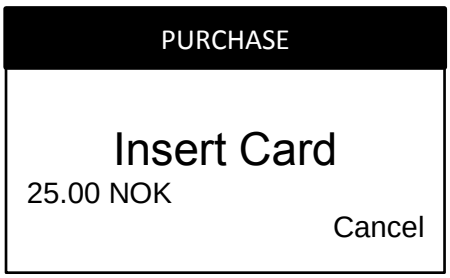
Possible issues

1. The transaction has exceeded maximum offline purchase limit.
2. The terminal has reached maximum number of stored offline transactions.
3. The card used has expired.
4. There is a communication issue with host, and the terminal has declined the transaction based on the communication error code. This code is only located in the debug log.
5. The transaction has been declined with a response code.
6. The transaction has been declined based on TVR and TSI.
7. There is something wrong with the keys in the terminal (i.e. online pin enciphering has failed)

Solution

1&2: Attempt to get the terminal online, by following the steps in “Troubleshooting offline ” chapter.
3: The terminal is offline and has declined the transaction because the card has expired. If a card has expired and the terminal is online, response code 54 should be present on the receipt.
4: Retry the transaction, it might be approved offline. Attempt to get the terminal online.
5: Locate the transaction in the response code list on page 38 and perform the “action” in the list.
6. Locate the TVR and TSI on the receipt and compare it to the TVR and TSI chapter on page 41 to find out if the transaction has been declined based on TVR and TSI.
7: Contact PayEx 2nd Line Support

All errors listed on the previous page will show the following screenshots:



Terminal requires that the card is inserted.

Application label is displayed

The terminal requests PIN input.

The terminal tries to send the transaction to host.

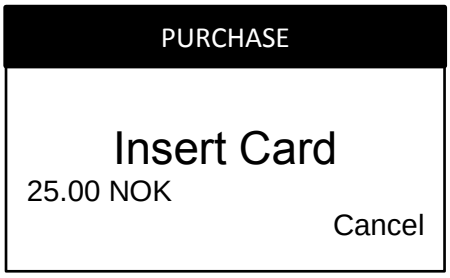
The transaction has been declined.

SSL is configured on the terminal, but the transactions are declined.

Possible errors and screenshots

1. The terminal is not configured correctly
2. The host connection and address might be wrong
3. SSL certificates are not loaded on the terminal correctly. Load new certificates.

Declined transactions with SSL will display the following screenshots:



Terminal requires that the card is inserted.

Application label is displayed

The terminal requests PIN input.

The terminal tries to send the transaction to host.

The transaction has been declined.

Solution

1: Verify that the SSL parameters are OK. Enter the support menu→Configuration Parameters→Set parameter. Input parameter “150” and press OK. This parameter shall be”1”. Input parameter “155” and press ok. This parameter shall be a password. Restart the terminal and retry the transaction if these parameters have been altered.

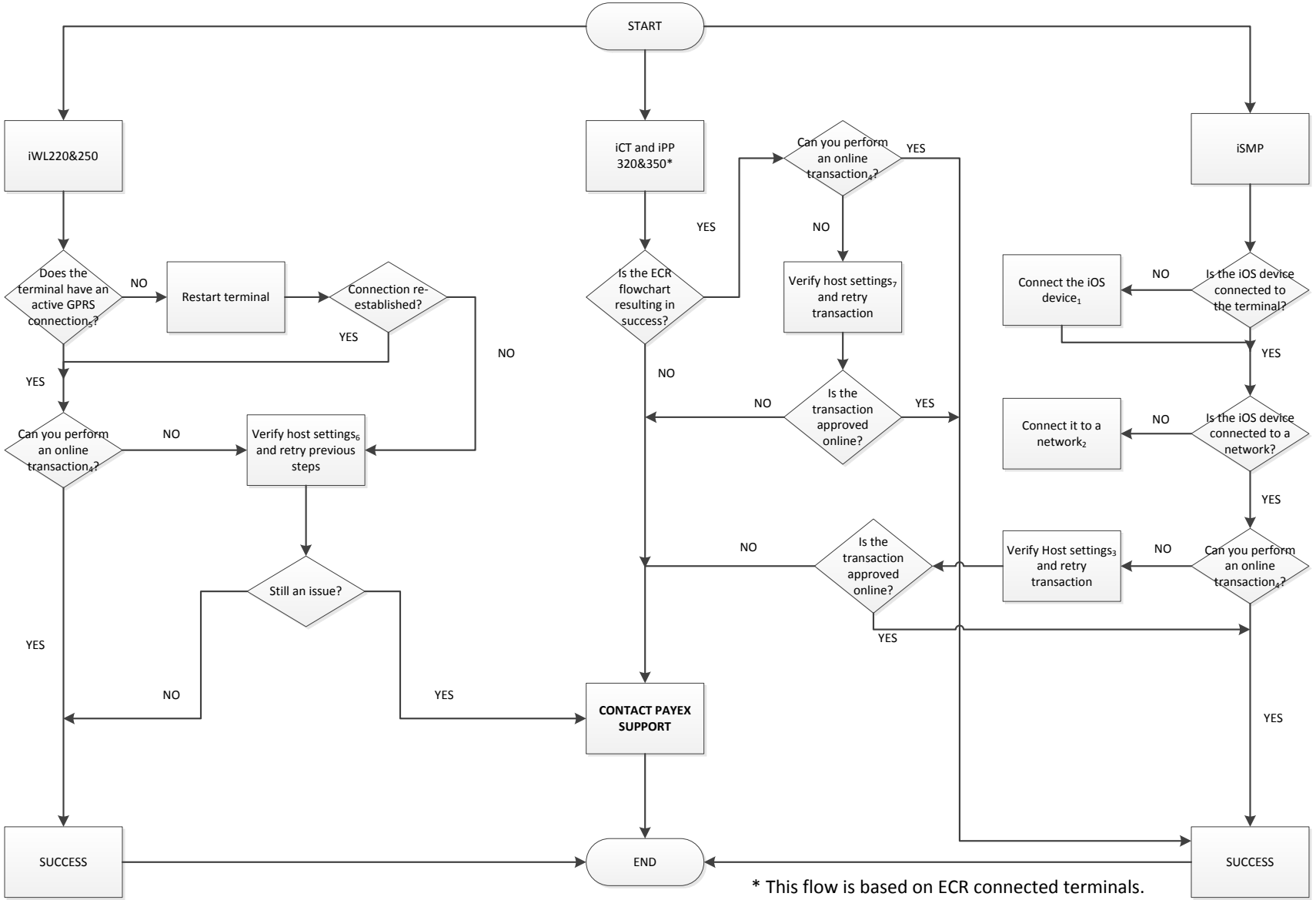
2&3: Contact PayEx 2nd Line Support.

Troubleshooting offline transactions

On the next page is a flowchart for offline terminals, and how to get them online.

1) Connect the iOS device:
    1. Connect the iOS device (iPod, iPhone) to the iOS device slot on the iSMP.
    2. Connect the iOS device to a Wi-Fi network. See 2).
    3. Start the payment application on the iOS device. Also make sure that the terminal is powered on.
2) Connect the iOS device to any Wi-Fi network (hotspot (ad-hoc) on a device, data connection on iPhone, wireless network access point).
3) Enter support menu→Settings→Host connection. Connection parameters shall be:
   With SSL:
   - IP address: pospaytx.payex.com and port: 443.
   Connection type: Ethernet.
4) A response code will be present on the receipt. See the example of receipts chapter on where to find the response code from host.
   Note that if the terminal has performed (several) offline transaction, this transaction may also be approved/declined offline. Please wait a while to let the terminal send offline transactions.
5) GPRS connection is active if a GPRS signal (bars) is displayed in the top left corner of the screen (iWL 250, opposite position on iWL 220), along with the SIM card name. The GPRS signal is optimal if five (5) bars is displayed. In addition, a phone connection must be active in the top center of the screen. It is not unusual that the phone connection is dropped if the terminal has been idle for a while. When sending a transaction after being idle, it shall re-establish the connection.
6) Enter support menu→Settings→Host connection.
   Connection parameters shall be:
   With SSL; IP address: pospaytx.payex.com, port: 443, GPRS apn is individual, based on what SIM card that is in use. Login and password are left blank.
   Connection type: GPRS.
   Without SSL: IP address: 195.225.0.42, port 9034, GPRS apn is individual, based on the SIM card. Login and password are left blank.
   Connection type: GPRS.
7) Depending on terminal setup, host settings shall be:
   PPP (USB) connected terminals:
   Connection parameters: IP address 1.1.1.1 and port 9034.
   Connection type: Ethernet
   Ethernet (LAN) connected terminals:
   Connection parameters:
   With SSL: IP address: pospaytx.payex.com, port: 443
   Without SSL: 195.225.0.42, port 9034 (*Or 9033*)

Troubleshooting offline terminals



* This flow is based on ECR connected terminals.

Other situations that will result in offline transactions:

DNS:

1. The terminal is configured with DNS address to host and:
    - The terminal is configured with static IP and DNS server is set wrong. The DNS server will never be found by the terminal, and therefore cannot translate the DNS address to an IP address.
    - The DNS server is unreachable.

   DNS errors can only be found in the Debug log. If DNS related issues are indicated, alter the host address to IP address. These are located in the Communication chapter.

Using the Telium manager

The Telium manager can be used to verify that a terminal has network connection. This is applied for all terminals, except iWL terminals.

- Enter the following key combination to enter the Telium menu:
  F3(up) + 1234 + Telium manager (0)
- **Ping a network address** to verify that the terminal has Internet connection:
  Initialization + Hardware + Ethernet setup + Ping. Enter a valid IP address and press OK/Enter. Received packages shall be 4/4.
- A terminal can be offline if the **boot protocol** is not configured correctly in the terminal. See the Parameters for terminals chapter on page 29.
- It is important that terminals configured with static IP has the right IP address, Gateway and DNS. See the Parameters for terminals chapter.

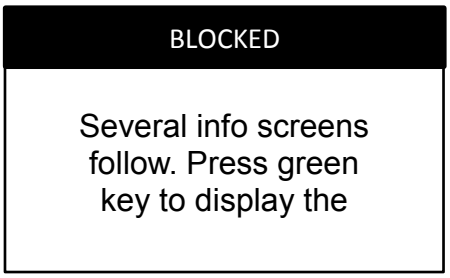
Blocked terminals

A terminal can be blocked in two ways:

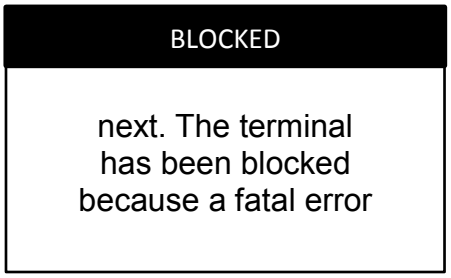
1. Transaction block – The terminal can be operated normally, except performing transactions.
2. Full block – The terminal will be fully blocked because a major incident has occurred on the terminal. The terminal will not be usable until it has been unblocked.

Warning! If a terminal gets blocked, contact PayEx 2nd Line Support immediately for further assistance.

The following screens will appear during terminal block. If it is a full block, the terminal will restart before displaying:

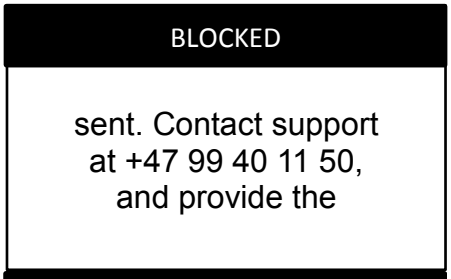


A blocked message will appear. Terminals with printer will print out terminal information that continues on the next info screens.



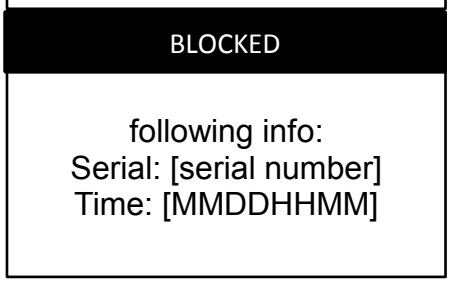
[press green key]

[press green key]



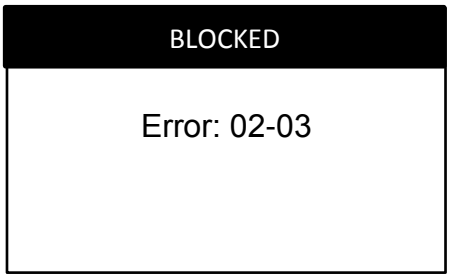
[press green key]

See Introduction chapter for correct phone number



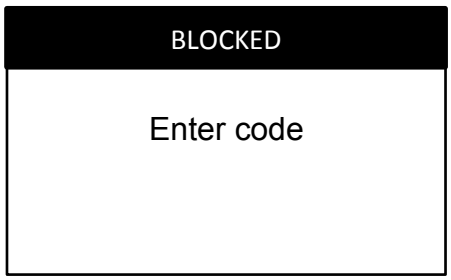
[press green key]

The serial number of the terminal will appear
The time will appear in format: Month, Month, Day, Day, Hour, Hour, Minutes, Minutes

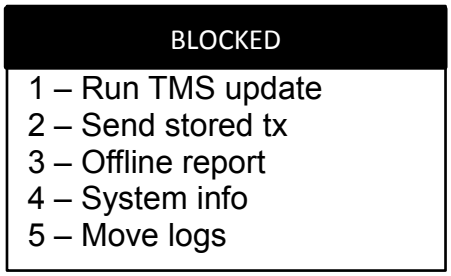


[press green key]

The error type will appear. In this example case, it is an offline approved transaction that has been sent, and host has responded with code 03 – Invalid merchant number.



Press green key and then press menu/F. This screen shall appear.
Enter the code provided by PayEx 2nd Line Support if requested to do so.



A blocked menu will appear. PayEx 2nd Line Support will advise which function to use.

A Transaction blocked terminal will display “TERMINAL BLOCKED” on the idle screen (start screen).
A “unblock” menu will appear below “support” in the menu where the unblock code can be entered.

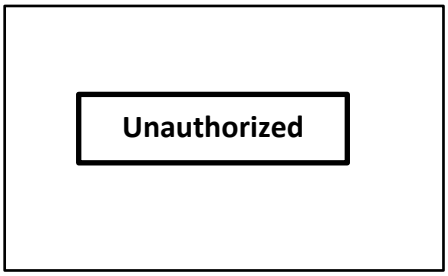
Terminal hardware errors

Alert irruption

If the terminal displays “Alert irruption!!!”, the terminal must be returned to PayEx. Contact PayEx 2nd Line Support if this screen appears on the terminal:

Unauthorized

If the terminal displays “Unauthorized”, the terminal must be returned to PayEx. Contact PayEx 2nd Line Support if this screen appears on the terminal:



Support menu

The support menu provides possibility to change settings and configuration.
In order to access the support menu, contact PayEx 2nd Line Support for a support code.
Note: A support menu password will only work for one day, attempting to access the support menu with the same password a different day will not work.

9-1 Settings

9-1-1 Setup ECR

Disable (Standalone operating mode)
Serial mode (Not used)
PPP mode (USB connection between ECR and terminal)
Ethernet mode (Ethernet connection between ECR and terminal)

9-1-2 TMS management

Configure (Sets the communication parameters for TMS connection)
Connect (Connects the terminal to TMS for downloading upgraded application and/or files)

9-1-3 Host connection

Connection parameters (Sets the address and port (and apn) to host)
Connection type (Select between Ethernet and GPRS)

9-2 Transaction list

Activate/Deactivate (Activate or deactivate transaction list)
Automatic print (Enable or disable automatic printing of transaction list). Automatic printing of transaction list will only be performed if the terminal is powered on and in idle mode(no transactions can be performed at this time). Automatic printing will automatically pause if the terminal run out of paper.

9-3 Configuration parameters

9-3-1 Print all parameters (Prints all parameters in the terminal)
9-3-2 Set parameter (Sets an existing parameter to a different value, or verifies that a parameter is correct)
9-3-3 Delete parameter (Deletes a parameter that is not in use)
9-3-4 Print EMV configuration (Prints EMV configuration on the terminal)

9-4 File management

9-4-1 List all files (Prints out the files on the terminal. Also asks for it to be stored on the HOST disk)
9-4-2 Delete sales report (Deletes current sales report)
9-4-3 Delete offline transactions (DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)
9-4-4 Delete total amount (Deletes total amount of the sales report)
9-4-5 Delete logs (Deletes the log file on the terminal)
9-4-6 Move logs (Moves the log files to the HOST disk. They can be recovered by using LLT)

9-5 Stored transactions

9-5-1 Print offline transactions

9-5-2 Delete offline transactions (DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)

9-5-3 Delete reversal (Deletes the reversal file (if any) on the terminal)

9-6 System info

9-6-1 System info (Displays and prints out system information; App version, Operating System and Telium system information

9-6-2 List components (Prints out components on the terminal)9-5-3 Security info (Prints out security information on the terminal)

9-6-2&9-6-3 are only applied if the terminal must be sent to PayEx for service.

9-7 Keys

9-7-1 Delete DUKPT keys (Deletes DUKPT keys on the terminal. DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)

9-7-2 Delete TGKIT keys (Deletes TGKIT keys on the terminal. Only applied if DUKPT keys are not loaded on the terminal. DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)

Files on the terminal

This chapter describes the files that can be loaded on a terminal with LLT. LLT is only applicable for 1st Line Support who has been provided this tool by PayEx.

HOST	SWAP
CONFIG	CONFIG.BIN[1]
EMV.PAR	***.AGN
BIN.CSV	***.M**
SALESREPORT	ISOCFG_0x.IC[1]
SURBINS	
SURCHARGES	
ISOCFG_0x.IC[1]	

CONFIG is the configuration file loaded on the terminal. See the Appendix E – Configuration parameters list chapter for a description of the content of this file.
EMV.PAR is a parameter file for all EMV cards. It includes i.e. currency codes, floor limits and TAC (information used for the terminal to accept the card online, offline or decline the card).
BIN.CSV is a file that contains the card agreements for each unique merchant and allowed transaction types for each card.
SALESREPORT is a file that can be loaded on the terminal, and stores performed transactions. This file is only loaded on standalone terminals.
SURBINS and SURCHARGES are two files that contain bin ranges and a fee percentage. These files are only used for merchants that perform transactions with surcharges.
ISOCFG_0x.IC and CONFIG.BIN are the same file and they format and verifies messages sent to host.
.AGN files are payment application files.
.M files are catalogue files that can be loaded locally with LLT. .M file endings are unique for each terminal type:

Terminal series	iCT 220&250	iPP320&350	iWL 220&250	iSMP
.M file ending	.M40	.M46	.M44	.M42

[1] CONFIG.BIN is loaded to the swap disk on terminals with 2.04 or prior application version. ISOCFG_0x.IC is loaded to the host disk on terminals with 2.05, 2.07 & newer, swap disk on 2.06c. x is the version of this file.

Communication

This chapter provides an overview of addresses, ports and settings for communication with TMS and host. This chapter describes the most used configuration for each terminal type.

TMS

All the terminals PayEx deliver are registered in TMS. TMS enables downloading of software, terminal Operating System, Manager, Keys and other files/applications.

Communication for TMS connection:
All PayEx terminal can connect to TMS for upgrading the terminal software/configuration. Two addresses can be used:

1. Open Internet: 91.208.214.34. All terminals that are connected to an open network shall use this address. Ports that can be used;
    a. 7003 – Clear port
    b. 7005 – PKI v3 port (C98 is displayed in the terminal window on startup)
    c. 7007 – PKI v1 port (A98 is displayed in the terminal window on startup)

2. Via PayEx private network: 195.225.0.45. All terminals that are connected to a private network (private APN for GPRS terminals) can perform TMS upgrade from this address. Ports that can be used;
    a. 9046 – Clear port
    b. 9048 – PKI v3 port
    c. 9050 – PKI v1 port

See the Troubleshooting TMS chapter for a step-by-step guide if the terminal is incapable of TMS update.

Parameters for terminals

iWL220&250

iWL communication parameters are based on the SIM card in the terminal.

Communication between host and terminal:

SIM Card	SSL	APN	Host address	Port	SSL parameters
Telenor (Norway)	NO	MDABETTERM	pospaydirecttx.payex.com (DNS) 195.225.0.42 (IP)	9034	150=0
Telenor (Norway)	YES	Internet	Pospaytx.payex.com (DNS) 195.225.28.97 (IP)	443	150=1 151=posterminal
Telenor SE	NO	Payex.apn.telenor.se	pospaydirecttx.payex.com 195.225.0.42	9034	
Telenor SE	YES	Internet.se or Internet.telenor.se	Pospaytx.payex.com 195.225.28.97	443	150=1 151=posterminal

Important note: SSL can only be used on open Internet APN's. Using SSL on other APN's will result in a communication error.

Communication parameters between TMS and terminal:

1. Navigate to the T.M.S settings by entering the following key combination:
   F3(up arrow) +password(1234) +0(Telium Manager) +3(Initialization) +1(Parameters)+ T.M.S
2. The following settings shall be:
   - TMS Access: **IP/GPRS**
   - Serial Link = **USB** (Only Bluetooth iWL(iWL 252))
   - SSL -PKI v1/3: **Yes**
   - Profile SSL-PKI v1/3: **INGETRUST**
   - IP address: **IP ADDRESS**
   - IP address –PKI v1/3: **See TMS chapter for correct IP address**
   - Port – PKI v1/3: **See the TMS chapter for correct port**
   - APN: **Set the same APN to TMS as to Host.**
   - Login: **Leave it blank**
   - Password: **Leave it blank**
   - TMS identifier: **0**
   - Protected download: **off**

TMS IP address and port for iWL has a general condition:

- If the terminal uses open Internet APN to host with SSL, the Open Internet address to TMS shall be used. If it uses a private APN to host, the PayEx private network address to TMS shall be used.

iPP320 &350

iPP parameters are based on ECR connection type.

Communication between host and terminal:

ECR Mode	SSL	Host address	Host port	SSL parameters:
PPP (USB)	NO	1.1.1.1	9034	150=0
PPP (USB)	YES	1.1.1.1	9034	150=1, 155=posterminal
Ethernet (LAN)	NO	pospaydirecttx.payex.com (DNS) 195.225.0.42 (IP)	9034	150=0
Ethernet (LAN)	YES	Pospaytx.payex.com (DNS) 195.225.28.97 (IP)	443	150=1 155=posterminal

Communication for iPP with Ethernet Connection:

iPP terminals that are using Ethernet (LAN) communication use either DHCP or Static address.

- Terminal with DHCP enabled receives automatically network settings from a server. No individual network parameters needs to be configured.
- Terminals with Static address enables must be manually configured:
    - F3(up) +password(1234) + Telium manager (0) + Initialization + Hardware + Ethernet setup + Boot Proto. Select **Static address**
    - Navigate back to Ethernet setup and select **IP address**. Input an IP address that is available on the network.
    - Navigate back to Ethernet setup and select **Subnet mask**. Input a valid subnet mask.
    - Navigate back to Ethernet setup and select **Gateway**. Input a valid gateway.
    - Navigate back to Ethernet setup and select **DNS1**. Input the address of the DNS server.

Warning! It is important for terminals configured with static IP that **all** the parameters are correct. If the terminal i.e. is configured with DNS address to host and DNS1 is set wrong, it will never connect to the DNS server, and a communication error will occur. **The terminal will therefore never get online.**

Communication between TMS and terminal:

1. PPP connected terminals shall use The Mynt menu for TMS update.
    - Verify that parameter 110 is set to 7003 and 111 is set to 1.1.1.1
2. Ethernet configured terminals can use both Telium Manager and the Mynt menu for TMS connection. However, the Mynt menu shall be used by default.

Communication parameters between TMS and terminal if Telium Manager is used:

1. Navigate to the T.M.S settings by entering the following key combination:
   F3(up arrow) +password(1234) +0(Telium Manager)+3(Initialization)+1(Parameters)+T.M.S
2. The following settings shall be:
    - TMS Access: **IP/Eth**
    - SSL -PKI v1/3: **Yes**
    - Profile SSL-PKI v1/3: **INGETRUST**
    - IP address: **IP ADDRESS**
    - IP address –PKI v1/3: **See TMS chapter for correct IP address**
    - Port – PKI v1/3: **See the TMS chapter for correct port**
    - TMS identifier: **0**
    - Protected download: **off**

iCT220&250

iCT parameters are based on ECR connection type.

ECR Mode	SSL	Host address	Host port	SSL parameters:
Standalone	NO	pospaydirecttx.payex.com (DNS) 195.225.0.42 (IP)	9034	150=0
Standalone	YES	Pospaytx.payex.com (DNS) 195.225.28.97 (IP)	443	150=1 155=posterminal
Ethernet (LAN)	NO	pospaydirecttx.payex.com (DNS) 195.225.0.42 (IP)	9034	150=0
Ethernet (LAN)	YES	Pospaytx.payex.com (DNS) 195.225.28.97 (IP)	443	150=1 155=posterminal

iCT terminals use Ethernet connection, configured with either DHCP or Static address.

- Terminal with DHCP enabled receives automatically network settings from a server. No individual network parameters needs to be configured.
- Terminals with Static address enables must be manually configured:
    - F3(up) +password(1234) + Telium manager (0) + Initialization + Hardware + Ethernet setup + Boot Proto. Select **Static address**
    - Navigate back to Ethernet setup and select **IP address**. Input an IP address that is available on the network.
    - Navigate back to Ethernet setup and select **Subnet mask**. Input a valid subnet mask.
    - Navigate back to Ethernet setup and select **Gateway**. Input a valid gateway.
    - Navigate back to Ethernet setup and select **DNS1**. Input the address of the DNS server.

Warning! It is important for terminals configured with static IP that **all** the parameters are correct. I.e. if the terminal is configured with DNS address to host and DNS1 is set wrong, it will never connect to the DNS server, and a communication error will occur. **The terminal will therefore never get online.**

Communication between TMS and terminal:

iCT terminals shall use The Mynt menu for TMS update.

- Verify that parameter 110 and 111 are set to the right values.

The iCT terminal can in addition to the Mynt menu use the Telium manager for TMS update.

Communication parameters between TMS and terminal if Telium Manager is used:

1. Navigate to the T.M.S settings by entering the following key combination:
   F3(up arrow)+0(Telium Manager)+3(Initialization)+1(Parameters)+T.M.S
2. The following settings shall be:
   - TMS Access: **IP/Eth**
   - SSL -PKI v1/3: **Yes**
   - Profile SSL-PKI v1/3: **INGETRUST**
   - IP address: **IP ADDRESS**
   - IP address –PKI v1/3: **See TMS chapter for correct IP address**
   - Port – PKI v1/3: **See the TMS chapter for correct port**
   - TMS identifier: **0**
   - Protected download: **off**

TMS IP address and port for iCT has a general condition:

- If the terminal uses open Internet to host with SSL, the Open Internet address to TMS shall be used. If it uses a private network (without SSL) to host, the PayEx private network address to TMS shall be used.

iSMP

iSMP terminals are standalone and shall use SSL.

ECR Mode	SSL	Host address	Host port	SSL parameters:
Standalone	YES	Pospaytx.payex.com (DNS) 195.225.28.97 (IP)	4413	150=1 155=posterminal

Communication between TMS and terminal:

iSMP terminals shall use The Mynt menu for TMS update.

- Verify that parameter 110 and 111 are set to the right values.

The iSMP terminal can in addition to the Mynt menu use the Telium manager for TMS update.

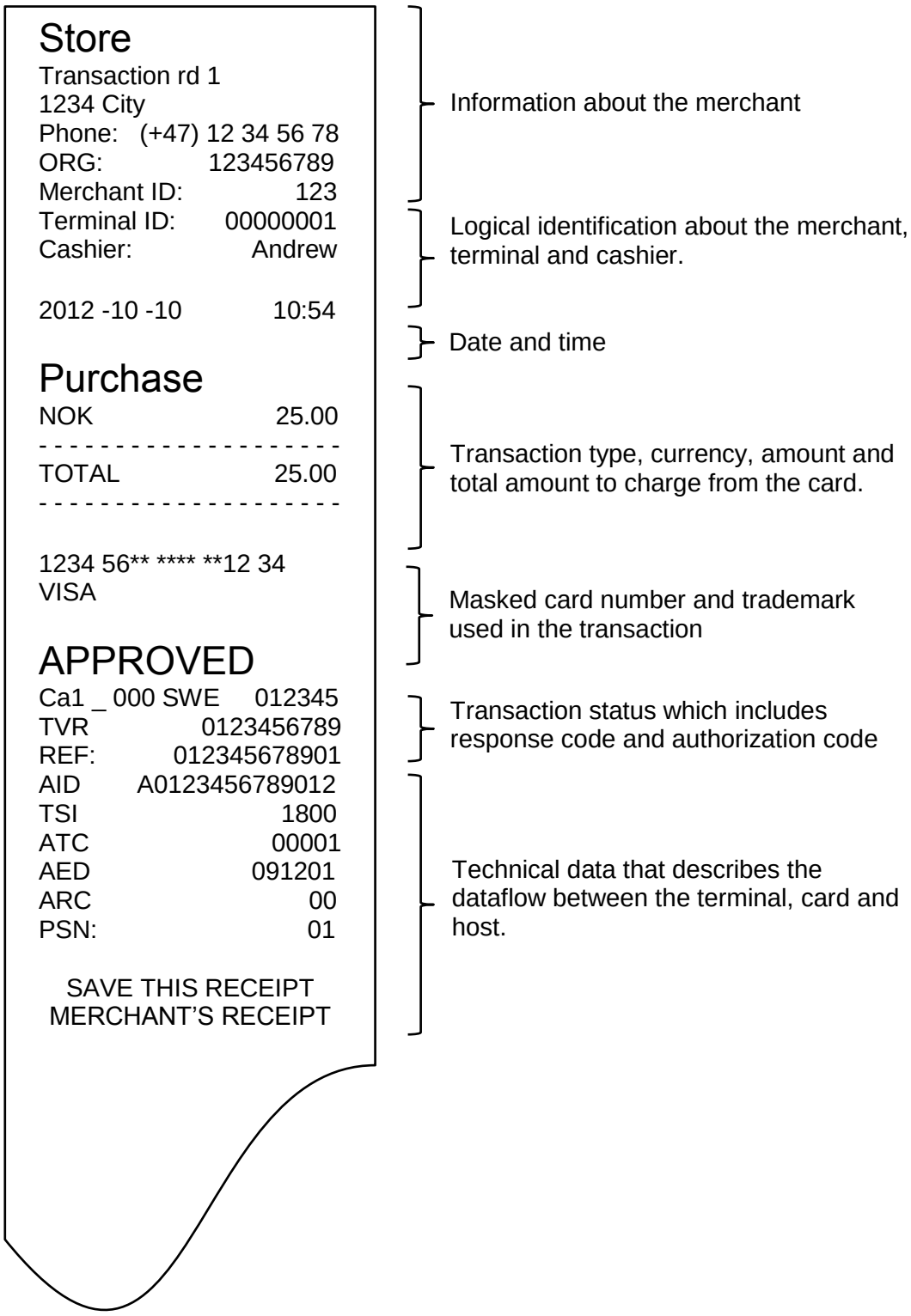
Communication parameters between TMS and terminal if Telium Manager is used:

3. Navigate to the T.M.S settings by entering the following key combination:
   F3(up arrow)+0(Telium Manager)+3(Initialization)+1(Parameters)+T.M.S
4. The following settings shall be:
   - TMS Access: **IP/Eth**
   - SSL -PKI v1/3: **Yes**
   - Profile SSL-PKI v1/3: **INGETRUST**
   - IP address: **IP ADDRESS**
   - IP address –PKI v1/3: **91.208.214.34**
   - Port – PKI v1/3: **7003**
   - TMS identifier: **0**
   - Protected download: **off**

Appendices

Appendix A – Receipt information

Approved purchase example


Store
Transaction rd 1
1234 City
Phone: (+47) 12 34 56 78
ORG: 123456789
Merchant ID: 123
Terminal ID: 00000001
Cashier: Andrew
2012 -10 -10 10:54
Purchase
NOK 25.00
- - - - - - - - - - - - - - - - - - - -
TOTAL 25.00
- - - - - - - - - - - - - - - - - - - -
1234 56** **** **12 34
VISA
APPROVED
Ca1 _ 000 SWE 012345
TVR 0123456789
REF: 012345678901
AID A0123456789012
TSI 1800
ATC 00001
AED 091201
ARC 00
PSN: 01
SAVE THIS RECEIPT
MERCHANT'S RECEIPT
Information about the merchant
Logical identification about the merchant, terminal and cashier.
Date and time
Transaction type, currency, amount and total amount to charge from the card.
Masked card number and trademark used in the transaction
Transaction status which includes response code and authorization code
Technical data that describes the dataflow between the terminal, card and host.

Translate the receipt information

Receipts generates information about the transaction performed. Before contacting PayEx 2nd Line Support, please translate as much information as possible before sending a support request. On the next page is an example of a declined transaction. A step by step breakdown of the information is described.

POS entry mode/Card data entry

Code		Entry Mode
Swedbank	NETS	
C	I	Chip
D	D	Magnetic Stripe
T	T	Key Entry
	E	Magnetic Stripe as fallback

Verification Method/CVM

Code		Verification Method
Swedbank	NETS	
@	@	Signature.
A	A	Online PIN (verified by host).
a	B	Offline PIN (verified by ICC).
/	C	CVM rule "No CVM Required" has been performed.
-	-	No CVM rule has been performed.
b	W	A combined CVM rule has been performed (Signature and Offline PIN)
[BLANK]	[BLANK]	Cardholder verification failed.

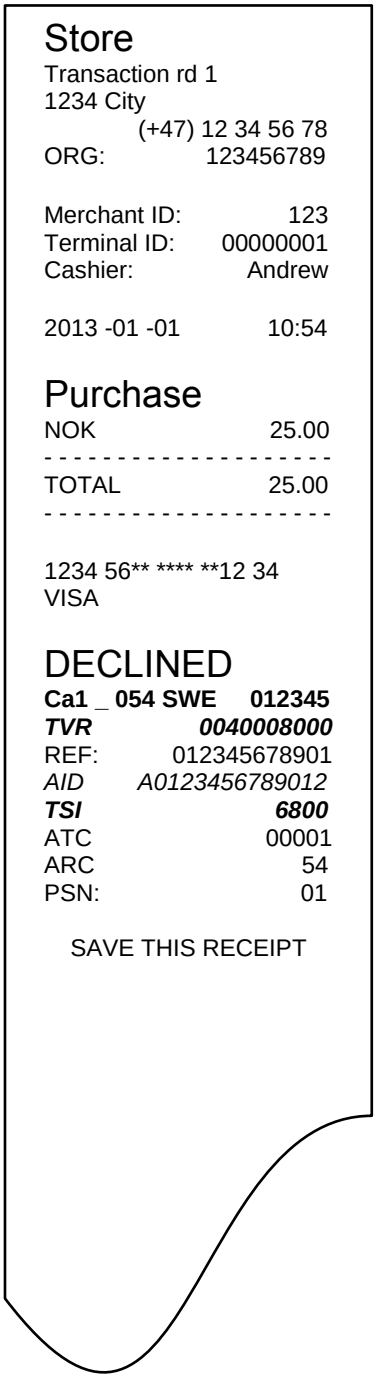
Card Authorization Channel

Code	Verification Method
1	Online
2	Swedbank: Offline, NETS: None
3	Swedbank: Offline PIN, NETS: Offline amount < floor limit
4	Phone
5	None (Always for Refund transactions)
-	Transaction declined before authorization

Card Authorization Responder (Swedbank only)

Code	Verification Method
1	Authorized locally in the terminal or terminal host system
3	Authorized by host
4	Authorized by host
5	Authorized by Card Issuer
6	Interchange interface process
7	Interchange (VISA or EPSS)
9	Authorized by merchant (acquiring host)
M	Approval code was manually entered
-	Transaction declined before authorization

Declined purchase example



Store
Transaction rd 1
1234 City
(+47) 12 34 56 78
ORG: 123456789

Merchant ID: 123
Terminal ID: 00000001
Cashier: Andrew

2013 -01 -01 10:54

Purchase
NOK 25.00
- - - - - - - - - - - - - - - - - - - -
TOTAL 25.00
- - - - - - - - - - - - - - - - - - - -

1234 56** **** **12 34
VISA

DECLINED
Ca1 _ 054 SWE 012345
TVR 0040008000
REF: 012345678901
AID A0123456789012
TSI 6800
ATC 00001
ARC 54
PSN: 01

SAVE THIS RECEIPT

Bold text is the transaction status. The 1st char is POS Entry Mode, 2nd is Verification Method, 3rd is Authorization Channel. In this example: C= Chip card, a=Offline PIN, 1= Online. Card Authorization channel is unknown, and response code is 054. SWE is an abbreviation for the financial institution, in this case SwedBank Babs.

Text with ***Bold italic*** is TVR and TSI. See Appendix C – TVR and TSI for a full description.

Italic text is AID; Application selected on the chip card. See Appendix D – AID.

Underlined text is the Application Response code. This is the same as in the transaction status, 54.

Conclusion:

Response code 54 means that the card has expired (see

Appendix B – Response codes). The TVR also specifies that the application has expired (see Appendix C – TVR and TSI).

The only option in this case is to request the customer to use a different card.

Appendix B – Response codes

This is a complete list of possible response codes from host.

If the response code can't be found in the table below, contact PayEx 2nd Line Support.

Response code	Response	Action
00	Transaction approved	
01	Transaction needs further authorization	Contact Acquiring Bank
03	Invalid merchant number	Contact Acquiring Bank
04	Declined	Use a different card
05	Declined	Use a different card
06	Declined	Use a different card
07	Declined	Use a different card
12	Declined	Use a different card
13	Invalid amount	Enter another amount
14	Invalid card	Use a different card
15	Card issuer not defined	Use a different card
17	Customer aborts card sequence	Retry transaction
19	Declined	Use another card
20	Transaction aborted	Retry transaction
25	Original transaction not found	Contact PayEx 2nd Line Support
29	Wrong session number	Contact PayEx 2nd Line Support
30	Format error	Contact PayEx 2nd Line Support
33	Card expired	Use a different card
34	Wrong CDV (check digit verification)	Retry transaction or use a different card
36	Declined	Use a different card
38	Number of possible PIN exceeded	Use a different card
39	Declined	Use a different card
41	Declined	Use a different card
43	Declined	Use a different card
51	Declined	Use a different card
54	Card expired	Use a different card
55	Wrong PIN	Retry PIN or use a different card
56	No card record	Use a different card
57	Service not allowed for acquirer	Transaction type not permitted. Contact PayEx 2nd Line Support
58	Service not allowed for the merchant	Transaction type not permitted. Contact PayEx 2nd Line Support
61	Refused by card issuer	Use a different card
62	Service not allowed for this card	Use a different card

63	CSN error (Security violation)	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
65	Too many transactions	Use a different card
67	Card blocked	Use a different card
68	Declined	Use a different card
75	Too many PIN attempts	Use a different card
77	Wrong MAC	Contact PayEx 2nd Line Support
80	Declined	Use a different card
81	Copied card	Use a different card
82	Wrong card format	Use a different card. Contact PayEx 2nd Line Support if this response code continues
83	Wrong session number	Contact PayEx 2nd Line Support
84	Reversal not possible, transaction declined	Contact PayEx 2nd Line Support
86	Duplicate transaction	Retry transaction
88	Missing PIN code	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
91	No contact with acquirer	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
95	Accumulator overflow	Contact PayEx 2nd Line Support
96	Error on Host	Retry the transaction. Contact PayEx 2nd Line Support if this is continuous
97	Timeout	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
98	Error in card	Use a different card
99	Invalid card	Use a different card
9A	Wrong time in terminal (+/- 15 min)	Retry the transaction. The terminal has updated the time after receiving this response code
9B	Declined – too many fallback attempts	Use a different card
9C	Card read error	Retry transaction
9D	Terminal blocked. Terminal must be upgraded.	Contact PayEx 2nd Line Support
A0	Error in card	Use a different card
A1	Card not found in card register	Use a different card
A3	Declined – Error in safety values	Use a different card
A9	Wrong EMV cryptogram	Contact PayEx 2nd Line Support
D2	EMV security error	Contact PayEx 2nd Line Support
D4	Cryptogram error	Contact PayEx 2nd Line Support

F1	Card Blacklisted	Use a different card
F2	Incorrect KID	Contact PayEx 2nd Line Support
F3	KID missing	Contact PayEx 2nd Line Support
FF	Declined	Use a different card
G5	Declined, magstripe on chipcard	Retry with chip or use a different card
G6	Invalid card – chip missing	Use a different card
J1	The bank does not have a bank access agreement	Contact PayEx 2nd Line Support
J2	The merchant does not have a bank access agreement	Contact PayEx 2nd Line Support
N0	The acquiring host is offline	Contact PayEx 2nd Line Support if this response code is continuous

Authorization response codes

The terminal generates response codes if the transaction performed is not authorized online.

Note: These response codes are printed only for terminal version 2.06 and newer & PosPay© client 4.9 and newer.

Value	Authorization Response code
Y1	Offline approved
Z1	Offline declined
Y3	Unable to go online, offline approved
Z3	Unable to go online, offline declined

Appendix C – TVR and TSI

TVR and TSI is a series of tests that the terminal performs when a chip card is inserted during a transaction. If the test fails, the transaction might be declined based on the TVR. TVR and TSI will always be present on the receipt when a chip card is used. In the "Detailed description/Impact" pane in the table below, there is a detailed technical description for each TVR BIT. Pay therefore notice to whether the transaction can or will be declined. Not all TVR BITS concludes whether the transaction will be declined. Contact PayEx 2nd Line Support for further instructions. See the example on page 44 on how to locate the TVR and extract the information. The cards accepted by the terminal have individual rules to what the transaction status shall be based on TVR and TSI. This overview provides only general information.

TVR

TVR BIT	Description	Detailed description/Impact
8000000000	*Offline data authentication was not performed*	**The transaction was not authenticated offline. Transaction is only authenticated online; otherwise signature is used as CVM. *Transactions will not be declined based on this TVR BIT by itself.***
4000000000	*SDA failed*	**Static Data Authentication failed**
2000000000	*ICC data missing*	**ICC data is missing.**
1000000000	*Card appears on terminal exception file*	**The card or an application on the card is blacklisted, and is not usable. The transaction will be declined**
0800000000	*DDA failed*	**Dynamic Data Authentication failed**
0400000000	*CDA failed*	**Combined Data Authentication failed**
0080000000	*ICC and terminal have different application versions*	**The terminal cannot find the application version on the card, or it's different than the terminal. *Transactions will most likely not be declined***
0040000000	*Expired application*	**The card has an expired application. Transactions will most likely be declined**
0020000000	*Application not yet effective*	**The application on the card is prior to the date from which the application may be used. Host decides transaction result**
0010000000	*Requested service not allowed for card product*	**Service not allowed. Transactions will be declined**

0008000000	*New card*	**The card has never performed an online transaction. *Transactions will not be declined***
0000800000	*Cardholder verification was not successful*	**CVM condition code was not recognized/known by the terminal. *Will most likely not result in a declined transaction***
0000400000	*Unrecognized CVM*	**Method number in the CVM code is not known, but CVM condition code is known. *Will most likely not result in a declined transaction***
0000200000	*PIN try limit exceeded*	**Number of PIN tries exceeded. The card will select available CVM methods or the terminal declines the transaction.**
0000100000	*PIN entry required and PIN pad not present or not working*	**Consecutive offline transactions with cards supporting only online PIN and signature will have this bit set. *Will most likely not result in a declined transaction***
0000080000	*PIN entry required, PIN pad present, but PIN was not entered*	**PIN was not entered. Will be present on Pin bypass transactions. *Will most likely not result in a declined transaction***
0000040000	*Online PIN entered*	**The card has online PIN. *Transactions will not be declined based on this TVR BIT by itself.***
0000008000	*Transaction exceeds floor limit*	**Transaction amount exceeds floor limit. The transaction must be verified online. *Transaction will not be declined if terminal is online.* Transactions may be declined if the terminal is offline**
0000004000	*Lower consecutive offline limit exceeded*	**Maximum number of consecutive offline transactions for this ICC application allowed in a terminal with online capability. Transactions will be declined.**

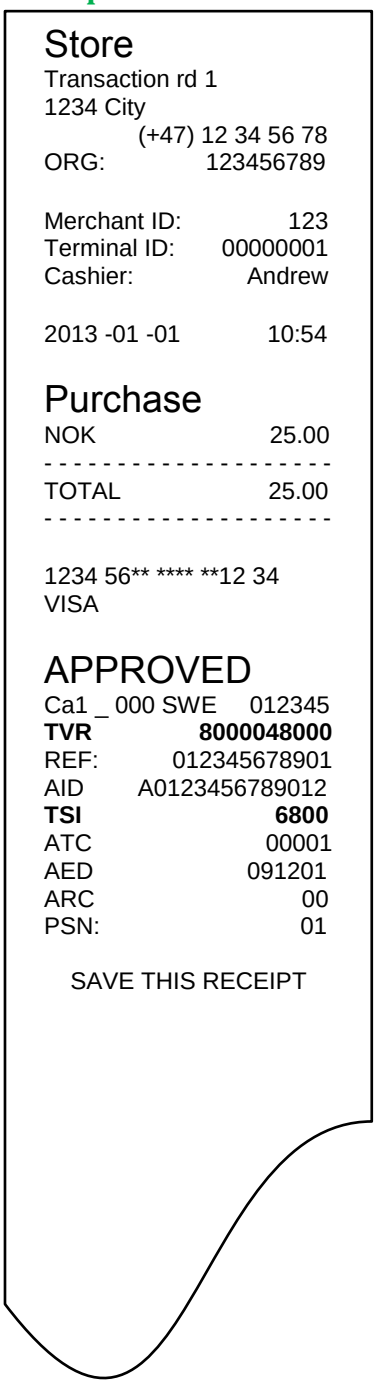
0000002000	*Upper consecutive offline limit exceeded*	**Maximum number of consecutive offline transactions for this application allowed in a terminal with offline capability. Transactions will be declined.**
0000001000	*Transaction selected randomly for online processing*	**The transaction is below floor limit, but it has been randomly selected for online processing. *Transactions will not be declined***
0000000800	*Merchant forced transaction online*	**Merchant forced the transaction online. Transactions will be declined if the terminal is offline**
0000000080	*Default TDOL used*	**Default TDOL is used by the terminal if the card does not provide a TDOL**
0000000040	*Issuer authentication failed*	**The card was not authenticated by the Issuer. Transactions will be declined**
0000000020	*Script processing failed before final GENERATE AC*	**Issuer script failed**
0000000010	*Script processing failed after final GENERATE AC*	**Issuer script failed**

TSI

The TSI on the receipt provides information about which of these tests that has been performed during a transaction. If multiple TSI tests have been performed, the TSI will have a hexadecimal value, from 0-F; see the example on the next page.

TSI BIT	Description
8000	*Offline data authentication was performed*
4000	*Cardholder verification was performed*
2000	*Card risk management was performed*
1000	*Issuer authentication was performed*
0800	*Terminal risk management was performed*
0400	*Script processing was performed*

Example



Store
Transaction rd 1
1234 City
(+47) 12 34 56 78
ORG: 123456789

Merchant ID: 123
Terminal ID: 00000001
Cashier: Andrew

2013 -01 -01 10:54

Purchase
NOK 25.00
- - - - - - - - - - - - - - - - - - - -
TOTAL 25.00
- - - - - - - - - - - - - - - - - - - -

1234 56** **** **12 34
VISA

APPROVED
Ca1 _ 000 SWE 012345
TVR **8000048000**
REF: 012345678901
AID A0123456789012
TSI **6800**
ATC 00001
AED 091201
ARC 00
PSN: 01

SAVE THIS RECEIPT

In this Example we can extract the information from the TVR:
8000000000 *Offline data authentication was not performed* – This bit will be set if the terminal cannot authenticate the card offline (i.e. the card has online PIN). The transaction is only verified online, or by signature if the terminal is offline.
0000040000 *Online PIN entered* – Online PIN was performed.
0000008000 *Transaction exceeds floor limit*- Some card schemes has 0 in Floor Limit. This means that all transactions must be approved online. If the terminal is offline, all transactions must be verified with signature. (It might be necessary to call the acquirer to request an authentication code as well).

From the TSI:
6000 6000 is not directly listed in the list of TSI. If multiple TSI tests have been performed, the TSI will have a hexadecimal value, from 0-F. In this case, **2000** – *"Card risk management was performed"* **AND 4000** – *"Cardholder verification was performed",* ***has been performed.***
0800 – *Terminal risk management was performed.*

Appendix D – AID

All EMV cards can contain multiple applications. Application selection is either automatically selected by the terminal when a customer inserts a card, or the customer selects the preferred application.

Card Scheme	RID	Product	PIX	AID
American Express	A000000025	American Express	01	A00000002501
BankAxept	D578000002	BankAxept	1010	D5780000021010
Dankort	A000000121	Debit card	1010	A0000001211010
Diners Club	A000000152	Diners Club	3010	A0000001523010
Discover	A000000152	Discover	3010	A0000001523010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060
VISA	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010

Appendix E – Configuration parameters list

This is a list of configuration parameters loaded on the terminal. Parentheses indicate the (maximum) length of the parameter. This is an example list, and is not valid for every terminal.

```
CLEAR;      // Used to clear all parameters already present on a terminal
16=578027;                  // (10) PSP code. Ignored by PayEx host but required
                                for IK loading
28=578;                     //  (3) Currency code. 578=no, 752=se, 208=dk.
36=00000010;                //  (8) Terminal ID.
43=995;                     // (10) Acquiring inst. ident.
60=PayEx;                    // (??) Merchant name.
61=Wergelandsvn 1;          // (??) Merchant address.
62=0167 Oslo;               // (??) Merchant address 2.
63=test-pospaydirecttx.payex.com; // (255) Host address (IP or hostname)
64=9034;                    //  (5) Host port (TCP)
65=NOK;                     //  (3) Currency text.
71=1234;                    //  (4) Supervisor password.
74=0;                       //  (1) Toggle: Tip.
75=55;                      //  (2) Tip limit as percentage.
77=1;                       //  (1) Toggle: Cents.
78=0;                       //  (1) Toggle: VAT.
79=25;                      //  (2) VAT percentage.
86=1;                       //  (1) Enable manual entry of PAN. Must always be set
                                To 1/0
96=1111;                    //  (4) Administrator password.
97=internet.telenor.se;     // (22) GPRS APN.
100=0;                      //  (1) Host connection type. Ethernet=0, GPRS=1.
                                MUST BE SET TO 1 FOR iWL TERMINALS!
109=0;                      //  (1) ECR mode. 0=off, 1=deprecated, 2=PPP,
                                3=ethernet.
110=9046;                   //  (4) TMS port.
111=195.225.0.45;           // (15) TMS IP.
112=internet.telenor.se;    // (22) TMS GPRS apn
115=0;                      //  (1) TMS connection type. Ethernet=0, GPRS=1.
                                MUST BE SET TO 1 FOR iWL TERMINALS!
116=2;                      //  (1) Track priority. Must be 2 or 3.
118=5;                      //  (3) Remember card notification sound: Seconds to
                                wait before sound starts
119=1;                      //  (1) Toggle: Remember card notification sound
120=1;                      //  (1) Toggle: Disable fallback
122=5;                      //  (4) Interval between offline transaction sending.
                                Minutes.
123=0;                      //  (1) Toggle: PIN/CVM before amount.
124=0;                      //  (1) Toggle: Add MAC process during loading IK.
125=COM5;                   //  (4) ECR communication interface
126=115200;                 //  (6) Baud rate.
127=1445;                   //  (4) Time for automatic TMS call.
130=0;                      //  (1) Require card present on manual reversal.
131=5541;                   //  (4) Merchant Category Code.
132=NO;                     //  (2) Terminal language as ISO 639-1 code.
133=1;                      //  (1) Toggle: Activate sending of events to ECR.
134=1;                      //  (1) Enable/Disable offline fallback. Set 1 to
                                disable offline fallback
135=(+47) 12 34 56 78;      // (17) Standalone receipts: Merchant phone number.
136=987654321;              //  (9) Standalone receipts: Merchant org. number.
137=Cashier;             // (12) Standalone receipts: Cashier name
138=3;                      //  (1) No. of allowed tries to enter Voice Auth Code.
```

```
140=D5780000021010;          // (14) If an AID is found, autoselect it. [0-F].
                                  BAX: D5780000021010, Dankort: A0000001211010
141=1;                       //  (1) Toggle: Print merchant copy when CVM is
                                  signature. Always Print mercant copy with no
                                  confirmation(Set in DK and IPA)
142=3;                       //  (3) Timeout for establishing TCP connection to host
143=10;                      //  (3) Timeout for sending data to host. 1-600 seconds
144=2;                       //  (1) DHCP on/off. 0=off, 1=on, 2=User controlled.
145=0;                       //  (3) Max amount for doing "No CVM" purchase.
146=0;                       //  (1) Enable surcharge on the terminal. 0=off, 1=on.
147=+47 99 40 11 50;         // (20) Phone number for support
148=0;                       //  (1) Toggle: Enable/Disable beeping on PIN entry
149=0;                       //  (1) Decline when call for auth 0=off, 1=on.
150=0;                       //  (1) Toggle: Enable/Disable SSL for HOST
151=3;                       //  (5) Remember card notification sound: Seconds to
                                  beep discreetly before loud sound
152=0100;                    //  (4) String with format 'HHMM' for setting time to
                                  print salesreport file
153=0;                       //  (1) Enable manual entry of [PosPay] value codes.
154=1;                       //  (1) Enable starting a sale transaction by pressing
                                  F2 and entering card information manually.
155=;                        // (64) Password for SSL client certificate
157=0;                       //  (1) Toggle: Enable/Disable sales Report
158=0;                       //  (1) Toggle: Disable purchase in standalone
159=0;                       //  (1) Toggle: Disable cashback in standalone
160=0;                       //  (1) Toggle: Disable reversal in standalone
161=0;                       //  (1) Toggle: Disable refund in standalone
162=0;                       //  (1) Toggle: Disable preauth in standalone
163=0;                       //  (1) Toggle: Disable completion in standalone
164=0;                       //  (1) Toggle: Disable balance in standalone
165=0;                       //  (1) Toggle: Disable withdrawal in standalone
166=0;                       //  (1) Toggle: Disable logging
167=1107;                    //  (4) Time to perform terminal time update.
168=1;                       //  (1) Toggle: Beep after a transaction
169=0;                       //  (1) Toggle: Mute terminal
171=0;                       //  (1) Toggle: Use GOAL
173=0;                       //  (1) Toggle: Enable the ECR flow step for
                                  preliminary transaction response
174=0;                       //  (1) Toggle: Manually activate/deactivate header and
                                  footer when using custom background
185=1;                       //  (1) Toggle: Enable amount confirmation when
                                  Tip/Surcharge is used
186=Have a nice day;         //(127) Greeting at end of receipt
187=5;                       //  (4) Number: Max offline transactions in terminal.
189=0100;                    //  (4) Time to print total user report
191=1;                       //  (1) Toggle: Allow NFC transactions
193=0;                       //  (1) Toggle: Use custom GOAL menu. 0=off, 1=on
195=0;                       //  (1) Toggle: Toggles beeping on all user input
196=9039;                    //  (4) NFC port.
197=0;                       //  (1) Toggle: Print receipts using BT-printer (0) or
                                  send to POS-app as HTML(1) (iSMP).
198=0;                       //  (1) Tips entry mode: 0=Enter total, 1=Enter tips
199=1;                       //  (1) Enable sending card info during ECR transaction
                                  flow.
201=1;                       //  (1) Enable/Disable sending ping/pong during ECR
                                  session.
```

```
204=1;                  //  (1) Toggle: Enable/Disable performing Wait for ECR
                                during ECR transaction flow.
206=0;                  //  (1) Toggle: Enable/Disable transaction list
207=0;                  //  (1) Enable/Disable automatic transaction list print
208=0300;               //  (4) Time to print transaction list.
209=1;                  //  (2) How often parameter list should be sent to
                                host.(hours) (0=disable)
210=1;                  //  (1) Toggle Roundup 0=disable, 1=enable
211=1;                  //  (1) Allow PIN-BYPASS (1=enable).
212=0;                  //  (1) Toggle: If GPRS monitoring shall be used
213=0;                  //  (1) Receipt standard: 0=Swedbank, 1= NETS
214=0;                  //  (1) Toggle: Prompt for posref in standalone preauth
215=0;                  //  (1) Timezone difference from CET
216=0;                  //  (1) Toggle: Display PAN when call for auth (ECR)
251=0;                  //  (1) Toggle: Use serial packet with PPP. DEPRECATED.
253=0;                  //  (1) Toggle: Make terminal use an old revision of
                                the ECR protocol, where some messages had non-
                                TLV-encoded data. DEPRECATED.
                                MUST BE SET TO 1 FOR POSPAY CLIENTS!
254=1;                  //  (1) Toggle: IPA_VERSION_1 = 1 IPA VERSION_2 = 0,
                                see ECR Interface  rev 0.68
255=0;                  //  (1) Toggle: Do not send EMV approval offline
                                response codes. Should be set to 1 for PosPay
                                4.8.x and earlier. DEPRECATED.
```

Appendix F – Supported schemes

Below is a list of supported cards by PayEx. Note that not all merchants support all cards listed below.

Card	Card
ACCEPTCARD	Metax
AgriCard (VISA)	NAF
Aktiiviraha	Neocard
Amagerkortet	Nets Kjedegavekort
American Express	Nets Sentergavekort
Aurinkomatkat	OoB-Card
BankAxept	OP-Kotipankki
Bankkort	Pankkikortti
Bankkort (Coop)	PayEx Gavekort
Bankkort (GE Kapital Bank)	PayEx Loyalty
Beoscan	PBS Centerkort
Blackhawk Gift cards and value codes	PBS Handelstand
Cashcomspresentkort	PBS Kjedekort
China Union Pay	PosPay Value cards and -codes
Coop Bonus	PREEM
COOP Mastercard	Resursbank
COOP Visa	RIK
Dankort	Rikslunchen
Diners Club	S-Business Card Manage
DKV	Sentrumsgavekort
Esso	S-Etu
Esso Fuel	Shell Mastercard
EuroShell	Shell Mastercard
EVC Gift cards and value codes	SKODA
FDM (Statoil)	S-Lahjakortit
FINAX GE CAPITAL	SOK Gift Card
Finnair	S-Pankki
Forbrugsforeningen	Spar kortti
Gavekort 1	SparXpres
Gavekort Kjede	Spotify
Gavekort Senter	ST1
Habbo	Stadium
Handelsbanken Finans	S-Tili
HB Finans	Stockmann
Hemtex	SVENSKE BANKKORT
Ikano	Taksikortti
Ikano kortet	Ticket Rikskortet
iTunes	Tiliraha
Japan Credit Bureau	Tradeka
JCB	Trumf
Käyttöluotto	Meritarahoitus 2S
Kicks	Union Tank
K-Luotto	Universal Presentkort
LIC Mastercard	Vardetryck
Lindex kortet	VISA
LO Favør	VISA Electron
Luottokunta	Volvokortet
Lyngby Storcenter Konto	VW
Maestro	WyWallet
MasterCard	yX

Appendix H – Accessories

Contact order.pos@payex.com to purchase these products.

Terminal type	Category	Product name/description	Product number
iWL2xx	PSU	Terminal monoplug (PSU via micro USB)	192010793
iWL2xx	PSU	Base monoplug (PSU via a Base)	192010579
iWL2xx	PSU	Car charger (via micro USB)	192013244
iWL2xx	PSU	Travel adapter (Use the Base PSU to directly charge the terminal)	296110863
iWL2xx	Battery	Li-ions Battery	295006044
iWL2xx	Cable	Ethernet cable 3m	293500052
iWL2xx	Cable	Modem cable	179900087
iWL2xx	Cable	USB cable, female to micro USB (Connect the terminal to a USB device)	296109807
iWL2xx	Cable	USB cable, male to micro USB (Connect the terminal to a USB Host)	296109815
iWL2xx	Base	Charging base	iWL200-01P1481A
iWL2xx	Base	Ethernet modem base	iWL200-01P1482A
iWL2xx	Base	Bluetooth Ethernet modem base	iWL200-01P1483A
iWL2xx	Misc.	Paper feeder iWL	192000053
iPP3xx	Cable	Ethernet cable with External PSU	Cable: 296 114 829 PSU: 192011109
iPP3xx	Cable	USB type A Powered straight cable	296100039
iPP3xx	Cable	Magic Box L2500S TWP IPP3xx	296121027
iCT2xx	Cable	Magic Box ICT (Cable alim eth modem rs x07)	293523360

Appendix I – Abbreviations and acronyms

AID – Application ID
APN – Access Point Name
DDA – Dynamic Data Authentication
DHCP – Dynamic Host Configuration Protocol
DUKPT – Derived Unique Key Per Transaction
ECR – Electronic Cash Register
EMV – Europay, Mastercard, VISA
Extra – Gratuity, Tips.
GPRS – General Packet Radio Service
IP – Internet Protocol
ISP – Internet Service Provider
LAN – Local Area Network
LLT – Local Loading Tool. Tool used for loading terminal(s) from PC.
MAC – Message Authentication Code
MCC – Merchant Category Code. MCC is located in parameter no. 131.
PIN – Personal Identification Number
PPP – Point to Point Protocol
PSU – Power Supply Unit
SIM – Subscriber Identity Method
SDA – Static Data Authentication
SSL – Secure Sockets Layer
TAC – Terminal Action Codes
TDOL – Transaction certificate Data Object List
TMS – Terminal Management System
TSI – Transaction Status Information
TVR – Terminal Verification Results
USB – Universal Serial Bus

Notes